GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

En alianza con

TD SYNNEX FORTINET

Edición °3924

CIBERINTELIGENCIA DE AMENAZAS

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABILIDADES	3	1	0
MALWARE	0	1	2
NOTICIAS DE CIBERSEGURIDAD	0	0	3

VULNERABILIDADES

Nueva vulnerabilidad crítica en Ivanti CSA explotada activamente

Ivanti ha alertado sobre una nueva vulnerabilidad crítica (CVE-2024-8963) en su Cloud Services Appliance (CSA), ya explotada por actores maliciosos. La vulnerabilidad se debe a una falla de recorrido de directorios, que permite a atacantes remotos sin autenticación acceder a funciones restringidas en sistemas vulnerables. Esta vulnerabilidad se explota en conjunto con CVE-2024-8190, una inyección de comandos en CSA. Ivanti recomienda aplicar el parche 519 y migrar a CSA 5.0 para evitar compromisos adicionales, ya que la versión 4.6 ha llegado a su fin de vida.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/ivanti-warns-of-another-critical-csa-flaw-exploited-in-attacks/

GitLab soluciona vulnerabilidad crítica de omisión de autenticación SAML

GitLab ha lanzado un parche para la vulnerabilidad crítica CVE-2024-45409, que afecta a las instalaciones autogestionadas de las ediciones Community y Enterprise. La falla se encuentra en las bibliotecas OmniAuth-SAML y Ruby-SAML, que GitLab utiliza para la autenticación SAML, permitiendo a un atacante eludir la autenticación con respuestas SAML manipuladas. Si explotada, podría permitir acceso no autorizado a la instancia de GitLab.

Se recomienda actualizar a las últimas versiones y habilitar la autenticación de dos factores (2FA) para aquellos que no se puedan actualizar inmediatamente como medida temporal.

Prioridad: 1 Crítico.

Ampliar información:

https://www.bleepingcomputer.com/news/security/gitlab-releases-fix-for-critical-saml-authentication-bypass-flaw/

Parche para vulnerabilidad crítica en VMware vCenter Server

VMware ha emitido un parche para corregir una vulnerabilidad crítica de desbordamiento de memoria en su servidor vCenter, identificada como CVE-2024-38812 (CVSS: 9.8). La vulnerabilidad permite la ejecución remota de código si un atacante envía un paquete especialmente diseñado al servidor afectado, lo que podría comprometer completamente el sistema. Investigadores de la competencia Matrix Cup descubrieron esta falla, junto con

otra escalada de privilegios, CVE-2024-38813 (CVSS: 7.5). Se recomienda actualizar a las versiones más recientes de VMware vCenter Server 8.0 y 7.0 para mitigar el riesgo.

Prioridad: 1 Crítico.

Ampliar información:

https://thehackernews.com/2024/09/patch-issued-for-critical-vmware.html

---

SolarWinds corrige vulnerabilidad crítica de ejecución remota de código (RCE) en ARM

SolarWinds ha lanzado un parche para corregir una grave vulnerabilidad en su herramienta *Access Rights Manager* (ARM), utilizada para gestionar y auditar los derechos de acceso de usuarios en sistemas TI. La vulnerabilidad (CVE-2024-28991) fue descubierta por el investigador Piotr Bazydlo de la *Zero Day Initiative* de Trend Micro. El fallo radica en la deserialización de datos no confiables, lo que permitiría a un atacante ejecutar código de manera remota en el sistema afectado si explota esta falla, incluso con autenticación requerida. Esto podría llevar a la toma de control total del sistema**.**

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/09/solarwinds-issues-patch-for-critical.html

---

Recomendaciones generales sobre vulnerabilidades:

- Mantener los sistemas operativos y aplicaciones actualizados conforme a información directamente desde fabricantes y/o desarrolladores oficiales.

- Emplear controles compensatorios si no se pueden aplicar las actualizaciones de inmediato.
- Establecer una política y un plan periódico de mitigación de vulnerabilidades.
- Utilizar soluciones de gestión de vulnerabilidades para priorizar y abordar las vulnerabilidades.
- Adquirir tecnologías para bloquear accesos maliciosos y explotaciones de vulnerabilidades conocidas y de día cero.
- Utilizar servicios de Ethical Hacking para identificar posibles superficies de ciberataque y proteger los datos sensibles.
- Implementar sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y firewalls de aplicaciones web.
- Realizar auditorías de seguridad y pruebas de penetración regularmente.
- Educar a los usuarios y al personal de TI sobre las mejores prácticas de seguridad cibernética.
- Establecer políticas de seguridad sólidas, como el uso de contraseñas seguras y la gestión adecuada de accesos y privilegios.

MALWARE

SambaSpy: Un Nuevo Malware Vinculado a Brasil Ataca Infraestructuras

Un nuevo malware conocido como SambaSpy, vinculado a grupos de hackers brasileños, ha sido descubierto por investigadores de seguridad. Este malware afecta principalmente a sistemas basados en Linux, aprovechando fallos en el servicio Samba (una implementación de protocolo de archivos de red). El grupo detrás de este ataque utiliza el malware para obtener acceso remoto a los sistemas, principalmente en organizaciones y empresas de América Latina. SambaSpy se propaga al explotar configuraciones vulnerables en servidores de archivos compartidos, permitiendo a los atacantes ejecutar comandos arbitrarios para obtener control sobre los sistemas comprometidos.

El malware fue identificado por investigadores de Lumen Black Lotus Labs, quienes detallan que SambaSpy es altamente sigiloso, utilizando técnicas avanzadas de ofuscación para evitar la detección por soluciones de seguridad tradicionales. Las recomendaciones incluyen asegurar configuraciones Samba, deshabilitar servicios innecesarios y mantener actualizados los sistemas.

Prioridad: 2 Urgente.

Ampliar información:

https://thehackernews.com/2024/09/new-brazilian-linked-sambaspy-malware.html

---

Operación global de malware roba información de usuarios de cripto y gamers

El grupo criminal "Marko Polo" ha lanzado una operación de malware dirigida a usuarios de criptomonedas y gamers. Detectado por Insikt Group de Recorded Future, este ataque se propaga mediante spearphishing, malvertising, y suplantación de marcas conocidas como Fortnite, Zoom o RuneScape. Distribuye múltiples familias de malware, incluyendo AMOS, Stealc y Rhadamanthys, con capacidad de robar contraseñas, datos de monederos cripto, y claves de WiFi. Los atacantes utilizan campañas de phishing en redes sociales, así como software falso para infectar dispositivos con Windows y macOS.

Para evitar ser víctima de este tipo de ataques, se recomienda solo descargar software de sitios oficiales, no seguir enlaces de desconocidos y mantener actualizado el software antivirus. También es fundamental habilitar la autenticación de dos factores, monitoreando las cuentas de criptomonedas regularmente para detectar posibles anomalías.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/global-infostealer-malware-operation-targets-crypto-users-gamers/

Hackers norcoreanos apuntan a sectores energético y aeroespacial con malware MISTPEN

El grupo de ciberespionaje norcoreano UNC2970, vinculado a Lazarus, ha sido detectado atacando a sectores energéticos y aeroespaciales mediante campañas de phishing relacionadas con ofertas laborales falsas. Este ataque utiliza un archivo PDF malicioso que solo puede abrirse con una versión troyanizada de Sumatra PDF, la cual instala el malware MISTPEN.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/north-korean-hackers-target-energy-and.html

---

Recomendaciones generales sobre Malware:

- Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad.
- Utilizar soluciones de seguridad confiables, como antivirus y firewalls, y mantenerlos actualizados.
- Implementar autenticación multifactor en cuentas y sistemas para agregar una capa adicional de seguridad.
- Educar a los usuarios sobre la importancia de no hacer clic en enlaces o adjuntos sospechosos en correos electrónicos o mensajes.
- Realizar copias de seguridad regulares de los datos importantes y guardarlas en un lugar seguro y fuera de línea.

- Evitar descargar software de fuentes no confiables y solo utilizar tiendas oficiales para obtener aplicaciones.
- Establecer políticas de contraseñas sólidas y cambiarlas regularmente.
- Limitar los privilegios de acceso para los usuarios y las cuentas, y solo otorgar los permisos necesarios.
- Monitorear de cerca la actividad de red y utilizar herramientas de detección de intrusiones.

NOTICIAS DE CIBERSEGURIDAD

Desmantelan red internacional de phishing dirigida a credenciales móviles

Europol, junto con agencias de España, Argentina, y otros países, desmanteló una red criminal internacional que utilizaba la plataforma iServer para el robo de credenciales móviles. Identificado por Group-IB, este servicio de phishing como servicio (PhaaS) facilitaba el desbloqueo de teléfonos robados a través de mensajes falsos que engañaban a las víctimas para que ingresaran sus datos. Se arrestaron a 17 personas y se incautaron 921 dispositivos.

Prioridad: 3 Importante.

Ampliar información:

https://thehackernews.com/2024/09/europol-shuts-down-major-phishing.html

---

Europol desmantela la plataforma encriptada Ghost utilizada por criminales

Europol, junto con agencias de nueve países, desmanteló la plataforma de mensajería encriptada "Ghost", usada por redes criminales para tráfico de drogas y lavado de dinero. La plataforma ofrecía comunicaciones ultra seguras, con pagos en criptomonedas y

autodestrucción de mensajes. La operación, identificada por Europol, llevó a 51 arrestos en múltiples países, incluyendo Australia, Irlanda y Canadá.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/europol-takes-down-ghost-encrypted-messaging-platform-used-for-crime/

Botnet chino infecta 260,000 routers y cámaras IP

Investigadores de Black Lotus Labs han identificado la botnet Flax Typhoon, vinculada a hackers patrocinados por el estado chino, que ha comprometido más de 260,000 dispositivos como routers y cámaras IP. Utilizando variantes del malware Mirai, esta botnet, activa desde 2020, apunta a infraestructuras críticas en EE. UU. y Taiwán. La amenaza es que estos dispositivos infectados pueden ser utilizados para lanzar ataques DDoS masivos. Se recomienda actualizar el firmware de dispositivos, además de reemplazar aquellos sin soporte activo para reducir riesgos.

Prioridad: 3 Importante.

Ampliar información:

https://www.bleepingcomputer.com/news/security/europol-takes-down-ghost-encrypted-messaging-platform-used-for-crime/